In the Claims:

Please amend the Claims as follows and without prejudice. This listing of Claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims

1. (CURRENTLY AMENDED) A method for ~~securely exchanging information items used to generate encryption keys~~ facilitating secure communications among at least two parties ~~using a public/private encryption key system~~ over a communication network, comprising:

~~each of said parties~~ retaining a first ~~an initial~~ private key and transmitting [[an]] a corresponding first initial public key and synchronizing indicator ~~corresponding information item~~;

~~used by each receiving party~~ using a received second public key and second synchronizing indicator in combination with said retained first private key to determine, and retain, ~~an initial~~ a first encryption key [[,]] ;

~~said method comprising the steps of: a.~~ determining a ~~next~~ second private key, a third public key and a ~~next~~ third synchronizing indicator ~~corresponding information item set~~, wherein said ~~next~~ second private key is retained with said first retained private key ~~among said retained next private keys~~;

[[b.]] encrypting at least said third synchronizing indicator ~~one element of said next information item~~ using [[an]] said first encryption key ~~selected from said retained encryption keys~~;

[[c.]] transmitting said third public key and encrypted third synchronizing indicator ~~information item over said network~~;

[[d.]] decrypting a received ~~encrypted information item element~~ fourth synchronizing indicator using said first encryption key ~~a private key selected from said retained private keys~~; and

[[e.]] determining a [[next]] second encryption key from said [[next]] second private key, a fourth public key and said ~~received~~ decrypted fourth synchronizing indicator ~~information item~~, wherein said [[next]] second encryption key is retained with said first encryption key ~~among said retained encryption keys~~.

2. (CURRENTLY AMENDED) The method as recited in claim 1 wherein [[steps a-e]] said determining a next private key and a next ~~corresponding~~ information item set, encrypting at least one element of said next information item set, transmitting said encrypted next information element, decrypting said received encrypted information item element; and, determining a next encryption key from said next private key and said decrypted information item are repeated until a known number of encryption keys are determined.

3. (CURRENTLY AMENDED) The method as recited in claim 1 wherein said information item element [[is]] comprises a public key.

4. (CURRENTLY AMENDED) The method as recited in claim 1 wherein said information item element [[is]] comprises a synchronizing indicator.

5. (ORIGINAL) The method as recited in claim 1 wherein the step of encrypting further comprises: selecting at least one of said retained encryption keys alternatively.

6. (ORIGINAL) The method as recited in claim 1, wherein the step of encrypting further comprises: selecting a known encryption key.

7. (ORIGINAL) The method as recited in claim 6 wherein said known encryption key is such that an output value is the same as an input value.

8. (ORIGINAL) The method as recited in claim 5 wherein said encryption keys are selected in a known sequence.

9. (ORIGINAL) The method as recited in claim 8 wherein said known sequence corresponds to an order of retention of said encryption keys.

10. (ORIGINAL) The method as recited in claim 8 wherein said known sequence corresponds to an order pre-selected by said parties.

Claims 11 - 28. (CANCELED)